

SECURITY PLAN

FOR

**MINOS Detector Data Acquisition and Detector
Control Systems**
[ID 1023]

Responsibility for the system and its operation as described in this plan is accepted by:

_____ **Date:**_____

Minor Application Coordinator

Elizabeth Buckley-Geer

_____ **Date:**_____

MINOS Co-Spokesperson

Stan Wojcicki

SYSTEM IDENTIFICATION

System Name/Title

Fermilab issues an identifier for each General Support System (GSS) and Minor Application (MA) of the form CSP (Computer Security Plan)- MA/GSS- Organization- Number. Fermilab identifier CSP- MA-1023 has been assigned to the system discussed throughout this security plan and will be referred to as ID.

System Type

This system is a MA and is contained in the General Computing Enclave.

OMB 53 Exhibit Information

This system is contained by OMB 53 Exhibit FNAL Other Experiments, 019-20-01-21-02-3057-00-109-026.

Responsible Organization

Fermi National Accelerator Laboratory
PO Box 500
Batavia, IL 60510

Information and Security Contact(s)

Near Detector

Title	Name	email	Telephone	Initials
MA Coordinator	Arthur Kreymer	kreymer@fnal.gov	630-840-4261	
System Manager DAQ system	Carl Metelko	c.j.metelko@rl.ac.uk	44-1235- 446265	
System Manager DCS system	Alec Habig	ahabig@umn.edu	218-726-7214	
System Manager gateway node	John Urish	urish@fnal.gov	630-840-3017	
GCSC	Joe Klemencic	jkleme@cfnal.gov	630-840-3311	
MINOS Run Coordinator	Nick Graf Carlos Escobar	grafnj@fnal.gov escobar@fnal.gov	630-840-2978 630-840-4519	
Management contact	MINOS Spokespersons	plunk@fnal.gov jthomas@fnal.gov	630-840-2392 630-840-2041	

Far Detector

Title	Name	email	Telephone	Initials
MA Coordinator	Arthur Kreymer	kreymer@fnal.gov	630-840-4261	
System Manager DAQ system	Carl Metelko	c.j.metelko@rl.ac.uk	44-1235- 446265	
System Manager DCS system	Alec Habig	ahabig@umn.edu	218-726-7214	
System Manager gateway node	Dave Saranen	saranen@fnal.gov	218-753-6611	
GCSC	Jerry Meier Dave Saranen	meier@fnal.gov saranen@fnal.gov	218-753-6611	
MINOS Run Coordinator	Nick Graf Carlos Escobar	grafnj@fnal.gov escobar@fnal.gov	630-840-2978 630-840-4519	
Management contact	MINOS Spokespersons	plunk@fnal.gov jthomas@fnal.gov	630-840-2392 630-840-2041	

System Operational Status

ID is in the Operational phase of its life-cycle.

General Description/Purpose

The primary purpose of ID is to provide the data acquisition and detector control for the MINOS experiment. The MINOS experiment is a long baseline neutrino experiment consisting of a Far Detector in Soudan, Minnesota and a Near detector at Fermilab. Each detector has a separate data acquisition and detector control system. The data acquisition system (DAQ) reads continuous streams of raw digitizations from the front-end detector electronics, applies software triggering algorithms and creates events which it then writes to a mass storage device. The detector control system (DCS) is used to control and monitor a number of detector components. It monitors the front-end electronics racks and controls the power to those racks as well as the power to the photomultiplier tubes. It monitors the environmental conditions in the experimental halls. It is also used to control and monitor the magnet. Both the systems provide monitoring and status information to the experimenters running the detectors. For simplicity we will refer to the Far Detector as FD and the Near Detector as ND.

System Description and Boundaries

ID is comprised of all processing, communications, storage, and related resources located in the MINOS Experimental Halls at Fermilab and Soudan. The system is comprised of data acquisition and network equipment as shown in the diagrams below:

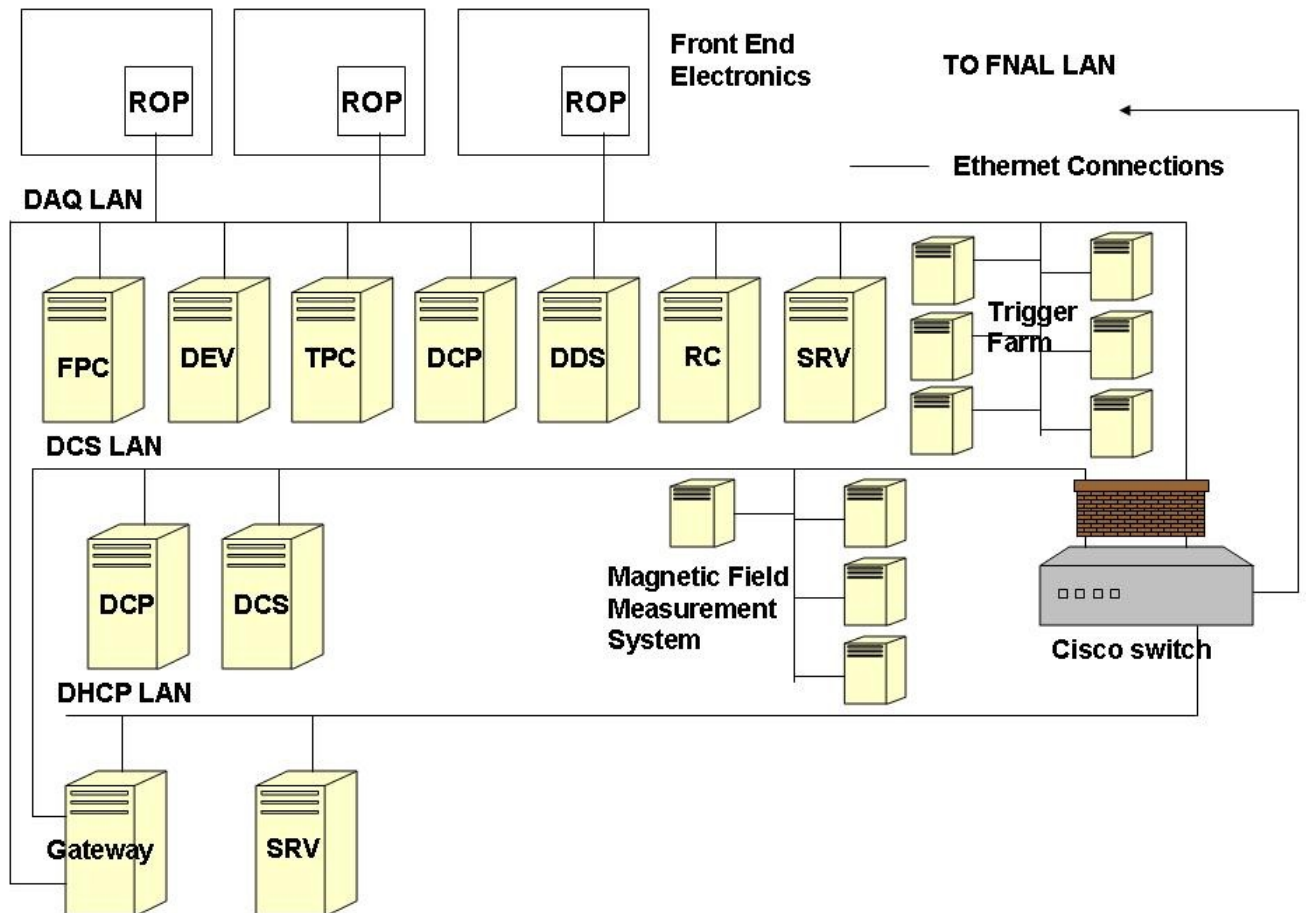


Fig. 1 Network diagram of the MINOS Near Detector Data Acquisition and Detector Control System

The Near Detector network consists of a single subnet partitioned into 3 VLANs with the following address ranges:

DHCP	131.225.192.192-222
DAQ	131.225.192.128-190
DCS	131.225.192.0-126

The Near Detector system is comprised of the following items:

Node Name	Function	Type of machine	OS
minos-gateway-nd	Login Gateway	PC	Linux
daqsrv-nd	Server for DAQ	PC	Linux
daqdev-nd	DAQ development machine	PC	Linux
daqdcp-nd	Data collection	PC	Linux
daqdds-nd	Data dispatcher	PC	Linux
daqrc-nd	Run Control	PC	Linux
daqfpc-nd	Light Injection Control	PC	Linux
daqtpc	Timing Control	PC	Linux
minossrv-nd	Local DAQ operation	PC	Linux
daqrop00-nd – daqrop07-nd	Read-Out Processors	VME board	VXWorks
daqbrp00-nd - daqbrp03-nd	Branch Read-Out Processors	PC	Linux
daqtp00-nd – daqtp05-nd	Trigger Processors	PC	Linux
daqpdu00-nd – daqpdu02-nd	Power distribution units		
daquds00-nd – daquds09-nd	Terminal server		
daqmcp-nd	Master Clock Processor	VME board	VXWorks
daqscs00-nd	Console server	Lantronix SCS3200	Linux
dcscdp-nd	Detector control	PC	Linux
bdotnd01-bdotnd04	Magnetic field measurement system	PC	Windows
fp-console	Environmental monitoring	PC	Windows

as shown in Fig. 1. In addition the system contains 39 BIRA Rack Protection units which each have an Ethernet connection.

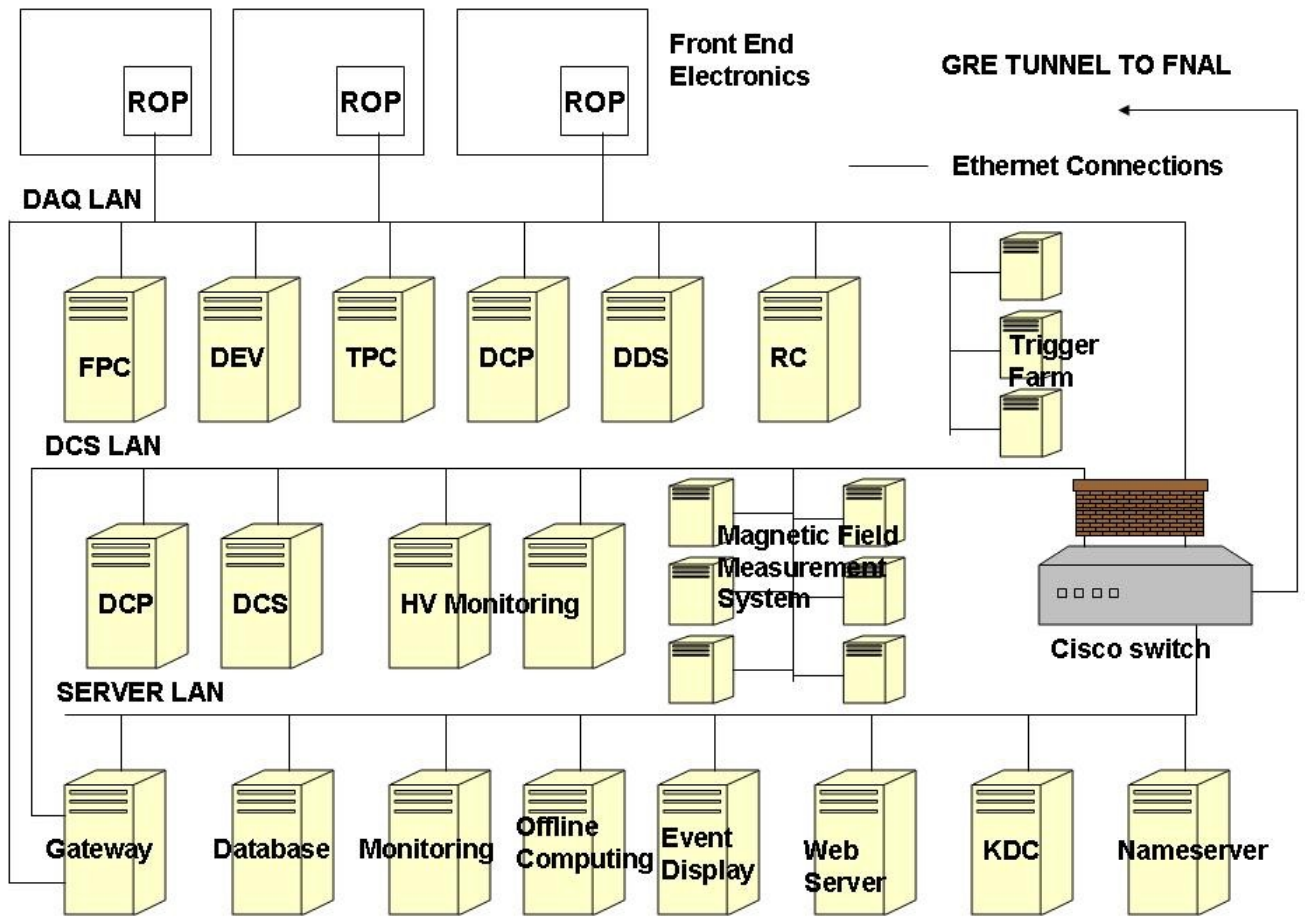


Fig. 2 Network diagram of the MINOS Far Detector Data Acquisition and Detector Control System

The Far Detector network consists of two subnets, one is used for DHCP and the other is partitioned into four VLANs (three are used by MINOS, the fourth is CDMS which is not covered by this document). The domain is minos-soudan.org. They have the following address ranges:

DHCP	198.124.212.0
SERVER	198.124.213.1-29
DAQ	198.124.213.129-253
DCS	198.124.213.65-125

The network at the Far Detector is configured and managed by the Fermilab Computing Division networking group. All network traffic from the FD LAN is sent to FNAL over a GRE tunnel and then routed to its final destination. All elements of the Fermilab CSPP apply to the network at the FD.

The Far Detector system is comprised of the following items:

Node Name	Function	Type of machine	OS
minos-gateway	Login Gateway	PC	Linux
daqsrv	Server for DAQ	PC	Linux
daqdev	DAQ development machine	PC	Linux
daqdcp	Data collection	PC	Linux
daqdds	Data dispatcher	PC	Linux
daqrc	Run Control	PC	Linux
daqfpc	Light Injection Control	PC	Linux
daqtpc	Timing Control	PC	Linux
daqrop00 – daqrop15	Read-Out Processors	VME board	VXWorks
daqbrp00 - daqbrp05	Branch Read-Out Processors	PC	Linux
daqtp00 – daqtp04	Trigger Processors	PC	Linux
daqpdu00 – daqpdu02	Power distribution units		
daquds00 – daquds15	Terminal server		
daqscs00	Console server	Lantronix SCS3200	Linux
dcscdp	Detector control	PC	Linux
bdot01-bdot07	Magnetic field measurement system	PC	Windows
dcs	Environmental monitoring	PC	Windows
dcshv1 – dcshv2	High Voltage Control & Monitoring	PC	Linux
minos-db	Database	PC	Linux
hydra	Local DAQ control	PC	Linux
minos-offline2	Offline computing system	PC	Linux
event1	Event Display	PC	Linux
farweb	Web Server	PC	Linux
i-krb-8	KDC	Sun	SunOS
fnsrvsm	Name Server	PC	Linux

as shown in Fig. 2. In addition the system contains 23 BIRA Rack Protection units and other low level control devices which have Ethernet connections. There are also 16 terminal servers.

System Environment

The Near detector system is physically located in the MINOS Near Detector Hall at Fermilab located approximately 400 feet below the surface and is accessed by an elevator. This area is occupied by employees, contractors, and registered users and is not open to the general public. Hard hats are required.

The Far detector system is physically located in the MINOS Far Detector Hall approximately 2300ft below the surface in the Soudan Underground Laboratory. It is accessed by an elevator. This area is occupied by employees, contractors, and registered users. The detector hall is visited by the public on twice daily escorted tours during the tourist season. They do not have access to areas containing computing equipment. Hard hats are required.

System Interconnection/Information Sharing

All connections are via the Fermilab network and are covered by Fermilab's Computer Security Protection Plan (CSPP). The network at the FD is considered an extension of the Fermilab network (see section 1.8 for the details) and is covered by the same CSPP.

Applicable Laws or Regulations Affecting the System

- OMB Circular A-130, "Management of Federal Information Resources," Appendix III, "Security of Federal Automated Information Resources," updated in 1996.
- OMB Circular A-11, Section 53, "Information Technology"
- Computer Security Act of 1987 (P.L. 100-235).
- Freedom of Information Act of 1986 (P.L. 99-570).
- FISMA
- Privacy Information Assessment required under the eGov act of 2002
 - DOE PCSP (Program Cyber Security Plan)
 - Fermilab CSPP (Computer Security Protection Plan)
 - Health Insurance Portability and Accountability Act of 1996. (HIPPA)

General Description of Information Sensitivity

Relative Importance of Protection Needs			
	HIGH (Critical Concern)	MEDIUM (Important Concern)	LOW (Minimum Concern)
Confidentiality			X
Integrity			X
Availability			X

Privacy Impact Assessment (PIA)

This system will not collect Personal Identification Information and no PIA is required.

Controls

The Fermilab CSPP includes the risk assessment addressing site wide threats and mitigations. A risk assessment must be performed on ID to identify system specific risks and mitigations. Similarly, the management, operational and technical controls from the CSPP are mandatory for all systems. This security plan for ID must identify those additional controls beyond those specified in the CSPP.

Risk Assessment and Management

A risk assessment has been conducted for ID to identify those areas not covered by the CSPP.

Review of Security Controls

- None to date.

Management Controls

The following management controls beyond those in the CSPP are implemented: None.

Operational Controls

The following operational controls beyond those in the CSPP are implemented: There are a small number of systems that should not be arbitrarily blocked by FCIRT without

consultation with the MA Coordinator or the MINOS Run Coordinator. These are described in the Incident Response Plan in Section 4.

Technical Controls

The DAQ and DCS LANs in Fig 1 and Fig. 2 contain VME processors and other devices that cannot use strong authentication. To address this we implement the following technical controls beyond those described in the CSPP. The controls apply to both the Near and Far Detectors unless noted otherwise.

- The DAQ and DCS LANs are located behind a firewall, as indicated in the diagram.
- Outside access to the DAQ and DCS LANs is provided by a login gateway located on the Server LAN at the FD and the DHCP LAN at the ND. The gateway is a computer containing three Ethernet interfaces, one connected to each LAN. This computer is running Scientific Linux and runs strong authentication. Access is limited to those users who need to access the DAQ and DCS computers. The systems running TightVNC. are behind the firewall so there is no direct access to them from the public internet. Access to these systems is via the login gateway using strong authentication. Once the user is logged in to the gateway they connect to the system running TightVNC using ssh and tunnel the display output back through the gateway to their machine.
- The routers are configured with reflexive ACLs that permit replies to traffic that originated from within the DAQ and DCS LANs.
- There are a limited number of holes punched in the firewall to allow direct access between certain machines inside the firewall with certain machines outside the firewall. These are listed below:

Far Detector

Machine	Port	Allow connections from	Reason
daqdcp,dcsdcp		131.225.13.27	Data transfer to STKen DCache
		131.225.13.66	Data Transfer to STKen DCache
		131.225.13.68	Data transfer to STKen DCache

The data transfer to DCache uses passive ftp but the reflexive ACLs have a default timeout of 300 seconds. This causes the control path connection to drop out. The timeout values can only be altered on a per-list basis. Rather than increase the time-out for all connections we choose to allow incoming connections through the firewall from the Dcache systems.

Near Detector

Machine	Allow connections from	Reason
daqtpc-nd	Daqtpc	Exchange timing information between FD and ND

A different router is used at the Near Detector and does not require explicit holes for the data transfer to DCache.

Testing Plan

1.1. Remote access

- For each system located behind the firewall an attempt is made to login to the systems using telnet and/or ssh using the appropriate user accounts. This test is repeated yearly.
- For systems running TightVNC an attempt is made to access the VNC server from outside the firewall. There are four systems running TightVNC, daqdev, daqdev-nd, dcs and fp-console. This test is repeated yearly.
- A yearly review of all user accounts on the login gateways is performed by the relevant system manager and the MA Coordinator. Any accounts that are no longer needed are retired.

1.2. ACL verification

- A yearly review of the ACLs on the routers is performed by the MINOS DataComm liaison and the MA Coordinator. Any un-needed connections will be removed and the removal documented.

2. Incident Response Plan

The systems identified in the section entitled “System Description and Boundaries” as the Login Gateways (minos-gateway and minos-gateway-nd) should not be disturbed during an incident without first consulting the MINOS Run Coordinator and the MA Coordinator as indicated in the table entitled “Information and Security Contact(s)”.